UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,671	08/10/2001	Russell Andrew Fink	00-4046	6412

32127 7590 04/20/2005

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQEO3H14
IRVING, TX 75038

EXAMINER	
TESLOVICH, TAMARA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/927,671	FINK ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *10 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *08.10.01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-52 are pending.

Double Patenting

Claim 16 of US Patent No. 6,826,684 contains every element of claims 10, 25, and 48 of the instant application and as such anticipates claims 10, 25, and 48 of the instant application.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11

F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claim 10, 25 and 48 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 16 of U.S. Patent No. 6,826,684. Although the conflicting claims are not identical, they are not patentably distinct from each other for the following reasons:

Applicant's "a network security system for securing packet header information of data packet communicated between a first enclave and a second enclave through a wide area network" is equivalent to Fink et al.'s "system for securely transmitting, on a WAN, packets between at least a first enclave LAN and a second enclave LAN".

Applicant's "first communication device" corresponds to Fink et al.'s "source bastion host", both of which are in communication with a first enclave and the wide area network, and both of which are adapted to receive data packets and translate

predetermined portions of the packet header information before transmitting the packet back onto the wide are network.

Applicant's "second communication device" corresponds to Fink et al.'s "receiving bastion host", both of which are in communication with a second enclave and the wide area network, and both of which are adapted to receive and restore the predetermined portions of the data packet and place the data packet onto the second enclave.

It would have been obvious to one having ordinary skill in the art at the time of the invention to utilize a source bastion host as a first communication device and a receiving bastion host as a second communication device within Applicant's network security system as described in Fink et al. in order to provide Applicant's system with increased security.

Objections - Specification

The disclosure is objected to because of the following informalities: Applicant's 'Background of the Invention' cites US Patent Application "METHOD AND APPARATUS FOR PROVIDING ADAPTIVE SELF-SYNCHRONIZED DYNAMIC ADDRESS TRANSLATION AS AN INTRUSION DETECTION SENSOR" but fails to provide the U.S. Patent Application Serial Number (09/928133). Applicant's 'Background of the Invention' also cites US Patent Application "SLIDING SCALE ADAPTIVE SELF-SYNCHRONIZED DYNAMIC ADDRESS TRANSLATION" but fails to

provide the U.S. Patent Application Serial Number (09/927979). Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-52 are rejected under 35 U.S.C. 102(e) as being anticipated by Caronni et al. (US Patent No. 6,507,908).

As per claim 1, Caronni discloses a network security apparatus for securing packet header information of a data packet, comprising:

a key exchanger adapted to derive a cipher key (see Caronni col.6 lines 52-62);

a translator adapted to translate predetermined portions of said packet header information according a cipher algorithm keyed by the cipher key (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24); and

a communication device adapted to communicate the data packet between a first enclave and a second enclave through a wide area network (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 2, Caronni discloses a network security apparatus as forth in Claim 1, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Caronni col.8 lines 13-24).

As per claim 3, Caronni discloses a network security apparatus as set forth in Claim 1, wherein said translator is adapted to queue the data packet until said key exchanger has derived the cipher key (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 4, Caronni discloses a network security apparatus as set forth in Claim 1, wherein said key exchanger further comprises:

a timer adapted to reset at a predetermined time interval, wherein said key exchanger derives the cipher key when said timer resets and the data packet present at said translator (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 5, Caronni discloses a network security apparatus as set forth in Claim 1, wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 6, Caronni discloses a network security information apparatus for securing packet header a data packet, comprising:

a random number generator adapted to generate a random number (Examiner note: It is well known in the art that SKIP utilizes a randomly generated traffic key);

a translator adapted to translate predetermined portions of said packet header information according to a cipher algorithm seeded by the random number;

a communication device adapted to communicate the data packet between a first enclave and a second enclave through a wide area network (see Caronni col.6 lines 52-62; col.8 lines 12-24).

As per claim 7, Caronni discloses a network security apparatus as set forth in Claim 6, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host (see Caronni col.7 lines 38-45).

As per claim 8, Caronni discloses a network security apparatus as set forth in Claim 6, further comprising:

a timer adapted to reset at a predetermined time interval, wherein said random number generator derives the random number when said timer resets and the data packet is received by said translator (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 9, Caronni discloses a network security apparatus as set forth in Claim 6, wherein the wide area network the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 10, Caronni discloses a network security system for securing packet header information of data packet communicated between a first enclave and a second enclave through a wide area network, the system comprising:

a first communication device in communication with a first network ("enclave") and a wide area network connecting the first communication device to a second communication device, said first communication device adapted to receive the data packet, translate predetermined portions of said packet header information and place the data packet on the wide area network (see Caronni col.4 lines 51-59; col.5 lines 16-19; col.5 lines 31-41); and

a second communication device in communication with a second network ("enclave") and the wide area network, said second communication device adapted to receive and restore the predetermined portions of the data packet and place the data packet onto the second network ("enclave") (see Caronni col.8 lines 12-24).

As per claim 11, Friedman discloses a network security system as set forth in Claim 10, wherein the predetermined portions comprise:

identity information that identifies a sending host within the first network ("enclave") and a receiving host within the second network ("enclave") (see Caronni col.7 lines 38-45).

As per claim 12, Caronni discloses a network security system as set forth in Claim 10, further comprising:

a key exchanger coupled to said first and second communication devices, adapted to derive a cipher key (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24); and

a timer electrically coupled to said key exchanger, adapted to reset at a predetermined time interval (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 13, Caronni discloses a network security system as set forth in Claim 12,

wherein said key exchanger derives the cipher key when said timer resets and the first communication device receives the data packet (see Caronni col.9 line 55 thru col.10 line 22);

wherein said first and second communication devices translate the predetermined portions of packet header information according to a cipher algorithm keyed by the cipher key (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24).

As per claim 14, Caronni discloses a network security system as set forth in Claim 12, wherein said first and second communication devices are adapted to queue the data packet until the key exchanger has derived the cipher key (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 15, Caronni discloses a network security system as set forth in Claim 10, wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 16, Caronni discloses a method for securing packet header information of a data packet, comprising:

deriving a cipher key (see Caronni col.6 lines 52-62);

translating predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24); and

communicating the data packet between a first enclave and a second enclave through a wide area network (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 17, Caronni discloses a method securing packet header information as set forth in Claim 16, wherein the predetermined portions packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave(see Caronni col.8 lines 13-24).

As per claim 18, Caronni discloses a method for securing packet header information as set forth in Claim 16 further comprising:

queuing the data packet until the cipher key has been derived (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 19, Caronni discloses a method for securing packet header information as set forth in Claim 16 further comprising:

deriving the cipher key at a predetermined time interval if the data packet to be communicated has been presented to said translating step (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 20, Caronni discloses a method for securing packet header information as set forth in Claim 16 wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 21, Caronni discloses a method for securing packet header information of a data packet, comprising:

generating a random number (Examiner note: It is well known in the art that SKIP utilizes a randomly generated traffic key);

translating predetermined portions of said packet header information according to a cipher algorithm seeded by the random number; and

communicating the data packet between a first enclave and a second enclave through a wide area network (see Caronni col.6 lines 52-62; col.8 lines 12-24).

As per claim 22, Caronni discloses a method for securing packet header information as set forth in Claim 21, wherein the predetermined portions of packet header further comprises:

identity information that identifies a sending host (see Caronni col.7 lines 38-45).

As per claim 23, Caronni discloses a method for securing packet header information as set forth in Claim 21, further comprising:

deriving the random number at predetermined time interval if the data packet to be communicated has been presented to said translating step (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 24, Caronni discloses a method for securing packet header information as set forth Claim 21, wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 25, Caronni discloses a method for securing packet header information of a data packet, comprising:

receiving the data packet at a first network communication device;

translating predetermined portions of packet header information;

sending the data packet to a second network ("enclave") through a wide area network;

receiving the data packet at a second communication device on the second network ("enclave");

translating the predetermined portions of the data packet at the second communication device; and

placing the data packet onto the second network ("enclave")

(see Caronni col.4 lines 51-59; col.5 lines 16-19; col.5 lines 31-41; col.8 lines 12-24).

As per claim 26, Caronni discloses a method for securing packet header information as set forth in Claim 25, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Caronni col.7 lines 38-45).

As per claim 27, Caronni discloses a method for securing packet header information as set forth in Claim 25, further comprising:

deriving a cipher key at a predetermined time interval if the data packet is presented to the first communication device (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24); and

translating the predetermined portions of packet header information for the data packet according to a cipher algorithm seeded by the cipher key (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24).

As per claim 28, Caronni discloses a method for securing packet header information as set forth in Claim 27, further comprising:

queuing the data packet until the cipher key has been derived (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 29, Caronni discloses a method for securing packet header information as set forth in Claim 25, wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 30, Caronni discloses a communication device adapted for processing packet header information of a data packet, the communication device being operable to:

derive a cipher key (see Caronni col.6 lines 52-62);

translate predetermined portions of said packet header information according a cipher algorithm keyed by the cipher key (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24); and

communicate the data packet between a first enclave and a second enclave through a wide area network (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 31, Caronni discloses a communication device as set forth in Claim 30, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Caronni col.8 lines 13-24).

As per claim 32, Caronni discloses a communication device as set forth in Claim 30, the communication device being further operable to queue the data packet until the cipher key has been derived (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 33, Caronni discloses a communication device as set forth in Claim 30, the communication device being further operable to derive the cipher key at a predetermined time interval if the data packet to be communicated has been generated (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 34, Caronni discloses a communication device as set forth in Claim 30, wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 35, Caronni discloses a communication device adapted for processing packet header information of a data packet, the communication device being operable to:

generate a random number (Examiner note: It is well known in the art that SKIP utilizes a randomly generated traffic key);

translate predetermined portions of said packet header information according to a cipher algorithm seeded by the random number; and

communicate the data packet between a first enclave and a second enclave through a wide area network (see Caronni col.6 lines 52-62; col.8 lines 12-24).

As per claim 36, Caronni discloses a communication device as set forth in Claim 35, wherein the predetermined portions of packet header further comprises:

identity information that identifies a sending host (see Caronni col.7 lines 38-45).

As per claim 37, Caronni discloses a communication device as set forth in Claim 35, the communication device further operable to derive the random number at predetermined time interval if the data packet to be communicated has been presented to the communication device (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 38, Caronni discloses a communication device as set forth in Claim 35, wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 39, Caronni discloses a device for securing packet header information of a data packet, comprising:

means for deriving a cipher key (see Caronni col.6 lines 52-62);

means for translating predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24); and

means for communicating the data packet between a first enclave and a second enclave through a wide area network (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 40, Caronni discloses a device for securing packet header information as set forth in Claim 39, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Caronni col.8 lines 13-24).

As per claim 41, Caronni discloses a device for securing packet header information as set forth in Claim 39, further comprising:

means for queuing the data packet until the cipher key has been derived (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 42, Caronni discloses a device for securing packet header information as set forth in Claim 39, further comprising:

means for deriving the cipher key at a predetermined time interval if the data packet to be communicated has been presented to said means for translating (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 43, Caronni discloses a device for securing packet header information as set forth in Claim 39, wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 44, Caronni discloses a device for securing packet header information of a data packet, comprising:

means for generating a random number (Examiner note: It is well known in the art that SKIP utilizes a randomly generated traffic key);

means for translating predetermined portions of said packet header information according to a cipher algorithm seeded by the random number; and

means for communicating the data packet between a first enclave and a second enclave through a wide area network (see Caronni col.6 lines 52-62; col.8 lines 12-24).

As per claim 45, Caronni discloses a device for securing packet header information as set forth in Claim 44, wherein the predetermined portions of packet header further comprises:

identity information that identifies a sending host (see Caronni col.7 lines 38-45).

As per claim 46, Caronni discloses a device for securing packet header information as set forth in Claim 44, further comprising:

means for deriving the random number at predetermined time interval if the data packet to be communicated has been presented to the means for translating (see Caronni col.9 line 55 thru col.10 line 22).

As per claim 47, Caronni discloses a device for securing packet header information as set forth in Claim 44, wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

As per claim 48, Caronni discloses a device for securing packet header information of a data packet, comprising:

means for receiving the data packet at a first communication device;

means for translating predetermined portions of packet header information;

means for sending the data packet to a second network ("enclave") through a wide area network;

means for receiving the data packet at a second communication device on the second network ("enclave");

means for translating the predetermined portions of the data packet at the second communication device;

means for placing the data packet onto the second network ("enclave")

(see Caronni col.4 lines 51-59; col.5 lines 16-19; col.5 lines 31-41; col.8 lines 12-24).

As per claim 49, Caronni discloses a device for securing packet header information as set forth in Claim 48, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Caronni col.7 lines 38-45).

As per claim 50, Caronni discloses a device for securing packet header information as set forth in Claim 48, further comprising:

means for deriving a cipher key at a predetermined time interval if the data packet to be communicated has been presented to the first communication device (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24); and

means for translating the predetermined portions packet header information for the data packet according to a cipher algorithm seeded by the cipher key (see Caronni col.6 lines 52-62; col.7 lines 32-37; col.8 lines 12-24).

As per claim 51, Caronni discloses a device for securing packet header information as set forth in Claim 50, further comprising:

means for queuing the data packet until the cipher key has been derived (ssee Caronni col.9 line 55 thru col.10 line 22).

As per claim 52, Caronni discloses a device for securing packet header information as forth in Claim 48, wherein the wide area network is the Internet (see Caronni col.5 lines 17-20; lines 31-35).

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5, 10-20, 25-34, 39-43, and 48-52 are rejected under 35 U.S.C. 102(b) as being anticipated by Friedman et al. (US Patent No. 5,757,924).

As per claim 1, Friedman discloses a network security apparatus for securing packet header information of a data packet, comprising:

a key exchanger adapted to derive a cipher key (see Friedman col.5 lines 31-36);

a translator adapted to translate predetermined portions of said packet header information according a cipher algorithm keyed by the cipher key (see Friedman col.5 lines 22-30; col.7 lines 59-61; col.11 lines 14-16); and

a communication device adapted to communicate the data packet between a first enclave and a second enclave through a wide area network (see Friedman col.7 lines 63-65).

As per claim 2, Friedman discloses a network security apparatus as forth in Claim 1, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Friedman col.11 lines 8-10).

As per claim 3, Friedman discloses a network security apparatus as set forth in Claim 1, wherein said translator is adapted to queue the data packet until said key exchanger has derived the cipher key (see Friedman col.5 lines 46-51).

As per claim 4, Friedman discloses a network security apparatus as set forth in Claim 1, wherein said key exchanger further comprises:

a timer adapted to reset at a predetermined time interval, wherein said key exchanger derives the cipher key when said timer resets and the data packet present at said translator (see Friedman col.8 lines 1-14).

As per claim 5, Friedman discloses a network security apparatus as set forth in Claim 1, wherein the wide area network is the Internet (see Friedman col.2 lines 31-33). (Examiner takes specific note of paragraphs 3 and 4 of Applicant's *Specifications* wherein Applicant provides sufficient evidence that it is well known in the art that the Internet is the largest WAN in existence and has become an integral part of the missions of a wide variety of organizations who connect their networks to the Internet in order to share information with the cyber world in general as well as remote organizations with which they interact).

As per claim 10, Friedman discloses a network security system for securing packet header information of data packet communicated between a first enclave and a second enclave through a wide area network, the system comprising:

a first network security device ("communication device") in communication with a first network ("enclave") and a processing circuit ("wide area network) connecting the first network security device to a second network security device ("communication device"), said first security device adapted to receive the data packet, translate predetermined portions of said packet header information and place the data packet on the processing circuit; and

a second network security device in communication with a second network ("enclave") and the processing circuit, said second communication device adapted to

receive and restore the predetermined portions of the data packet and place the data packet onto the second network ("enclave") (see Friedman col.5 lines 15-30).

As per claim 11, Friedman discloses a network security system as set forth in Claim 10, wherein the predetermined portions comprise:

identity information that identifies a sending host within the first network ("enclave") and a receiving host within the second network ("enclave") (see Friedman col.6 lines 20-21). (Please note that Friedman specifically discloses encoding TCP packets which are well known in the art to include TCP headers comprising source and destination information such as port numbers).

As per claim 12, Friedman discloses a network security system as set forth in Claim 10, further comprising:

a key exchanger coupled to said first and second communication devices, adapted to derive a cipher key (see Friedman col.5 lines 31-36); and

a timer electrically coupled to said key exchanger, adapted to reset at a predetermined time interval (see Friedman col.8 lines 1-14).

As per claim 13, Friedman discloses a network security system as set forth in Claim 12,

wherein said key exchanger derives the cipher key when said timer resets and the first communication device receives the data packet (see Friedman col.8 lines 1-14),

wherein said first and second communication devices translate the predetermined portions of packet header information according to a cipher algorithm keyed by the cipher key (see Friedman col.5 lines 22-30; col.7 lines 59-61; col.11 lines 14-16).

As per claim 14, Friedman discloses a network security system as set forth in Claim 12, wherein said first and second communication devices are adapted to queue the data packet until the key exchanger has derived the cipher key (see Friedman col.5 lines 46-51).

As per claim 15, Friedman discloses a network security system as set forth in Claim 10, wherein the wide area network is the Internet (see Friedman col.2 lines 31-33). (Examiner takes specific note of paragraphs 3 and 4 of Applicant's *Specifications* wherein Applicant provides sufficient evidence that it is well known in the art that the Internet is the largest WAN in existence and has become an integral part of the missions of a wide variety of organizations who connect their networks to the Internet in order to share information with the cyber world in general as well as remote organizations with which they interact).

As per claim 16, Friedman discloses a method for securing packet header information of a data packet, comprising:

deriving a cipher key (see Friedman col.5 lines 31-36);

translating predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key (see Friedman col.5 lines 22-30; col.7 lines 59-61; col.11 lines 14-16); and

communicating the data packet between a first enclave and a second enclave through a wide area network (see Friedman col.7 lines 63-65).

As per claim 17, Friedman discloses a method securing packet header information as set forth in Claim 16, wherein the predetermined portions packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Friedman col.11 lines 8-10).

As per claim 18, Friedman discloses a method for securing packet header information as set forth in Claim 16 further comprising:

queuing the data packet until the cipher key has been derived (see Friedman col.5 lines 46-51).

As per claim 19, Friedman discloses a method for securing packet header information as set forth in Claim 16 further comprising:

deriving the cipher key at a predetermined time interval if the data packet to be communicated has been presented to said translating step (see Friedman col.8 lines 1-14).

As per claim 20, Friedman discloses a method for securing packet header information as set forth in Claim 16 wherein the wide area network is the Internet (see Friedman col.2 lines 31-33). (Examiner takes specific note of paragraphs 3 and 4 of Applicant's *Specifications* wherein Applicant provides sufficient evidence that it is well known in the art that the Internet is the largest WAN in existence and has become an integral part of the missions of a wide variety of organizations who connect their networks to the Internet in order to share information with the cyber world in general as well as remote organizations with which they interact).

As per claim 25, Friedman discloses a method for securing packet header information of a data packet, comprising:

receiving the data packet at a first network security ("communication") device;

translating predetermined portions of packet header information;

sending the data packet to a second network ("enclave") through a processing circuit ("wide area network");

receiving the data packet at a second network security ("communication") device on the second network ("enclave");

translating the predetermined portions of the data packet at the second network security ("communication") device; and

placing the data packet onto the second network ("enclave")

(see Friedman col.5 lines 15-30).

As per claim 26, Friedman discloses a method for securing packet header information as set forth in Claim 25, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Friedman col.6 lines 20-21). (Please note that Friedman specifically discloses encoding TCP packets which are well known in the art to include TCP headers comprising source and destination information such as port numbers).

As per claim 27, Friedman discloses a method for securing packet header information as set forth in Claim 25, further comprising:

deriving a cipher key at a predetermined time interval if the data packet is presented to the first communication device (see Friedman col.5 lines 31-36; col.8 lines 1-14); and

translating the predetermined portions of packet header information for the data packet according to a cipher algorithm seeded by the cipher key (see Friedman col.5 lines 22-30; col.7 lines 59-61; col.11 lines 14-16).

As per claim 28, Friedman discloses a method for securing packet header information as set forth in Claim 27, further comprising:

queuing the data packet until the cipher key has been derived (see Friedman col.5 lines 46-51).

As per claim 29, Friedman discloses a method for securing packet header information as set forth in Claim 25, wherein the wide area network is the Internet (see Friedman col.2 lines 31-33). (Examiner takes specific note of paragraphs 3 and 4 of Applicant's *Specifications* wherein Applicant provides sufficient evidence that it is well known in the art that the Internet is the largest WAN in existence and has become an integral part of the missions of a wide variety of organizations who connect their networks to the Internet in order to share information with the cyber world in general as well as remote organizations with which they interact).

As per claim 30, Friedman discloses a communication device adapted for processing packet header information of a data packet, the communication device being operable to:

derive a cipher key (see Friedman col.5 lines 31-36);

translate predetermined portions of said packet header information according a cipher algorithm keyed by the cipher key (see Friedman col.5 lines 22-30; col.7 lines 59-61; col.11 lines 14-16); and

communicate the data packet between a first enclave and a second enclave through a wide area network (see Friedman col.7 lines 63-65).

As per claim 31, Friedman discloses a communication device as set forth in Claim 30, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Friedman col.11 lines 8-10).

As per claim 32, Friedman discloses a communication device as set forth in Claim 30, the communication device being further operable to queue the data packet until the cipher key has been derived (see Friedman col.5 lines 46-51).

As per claim 33, Friedman discloses a communication device as set forth in Claim 30, the communication device being further operable to derive the cipher key at a predetermined time interval if the data packet to be communicated has been generated (see Friedman col.8 lines 1-14).

As per claim 34, Friedman discloses a communication device as set forth in Claim 30, wherein the wide area network is the Internet (see Friedman col.2 lines 31-33). (Examiner takes specific note of paragraphs 3 and 4 of Applicant's *Specifications* wherein Applicant provides sufficient evidence that it is well known in the art that the Internet is the largest WAN in existence and has become an integral part of the missions of a wide variety of organizations who connect their networks to the Internet in

order to share information with the cyber world in general as well as remote organizations with which they interact).

As per claim 39, Friedman discloses a device for securing packet header information of a data packet, comprising:

means for deriving a cipher key (see Friedman col.5 lines 31-36);

means for translating predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key (see Friedman col.5 lines 22-30; col.7 lines 59-61; col.11 lines 14-16); and

means for communicating the data packet between a first enclave and a second enclave through a wide area network (see Friedman col.7 lines 63-65).

As per claim 40, Friedman discloses a device for securing packet header information as set forth in Claim 39, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Friedman col.11 lines 8-10).

As per claim 41, Friedman discloses a device for securing packet header information as set forth in Claim 39, further comprising:

means for queuing the data packet until the cipher key has been derived (see Friedman col.5 lines 46-51).

As per claim 42, Friedman discloses a device for securing packet header information as set forth in Claim 39, further comprising:

means for deriving the cipher key at a predetermined time interval if the data packet to be communicated has been presented to said means for translating (see Friedman col.8 lines 1-14).

As per claim 43, Friedman discloses a device for securing packet header information as set forth in Claim 39, wherein the wide area network is the Internet (see Friedman col.2 lines 31-33). (Examiner takes specific note of paragraphs 3 and 4 of Applicant's *Specifications* wherein Applicant provides sufficient evidence that it is well known in the art that the Internet is the largest WAN in existence and has become an integral part of the missions of a wide variety of organizations who connect their networks to the Internet in order to share information with the cyber world in general as well as remote organizations with which they interact).

As per claim 48, Friedman discloses a device for securing packet header information of a data packet, comprising:

means for receiving the data packet at a first network security ("communication") device;

means for translating predetermined portions of packet header information;

means for sending the data packet to a second network ("enclave") through a processing circuit ("wide area network");

means for receiving the data packet at a second network security ("communication") device on the second network ("enclave");

means for translating the predetermined portions of the data packet at the second network security ("communication") device;

means for placing the data packet onto the second network ("enclave")

(see Friedman col.5 lines 15-30).

As per claim 49, Friedman discloses a device for securing packet header information as set forth in Claim 48, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave (see Friedman col.6 lines 20-21). (Please note that Friedman specifically discloses encoding TCP packets which are well known in the art to include TCP headers comprising source and destination information such as port numbers).

As per claim 50, Friedman discloses a device for securing packet header information as set forth in Claim 48, further comprising:

means for deriving a cipher key at a predetermined time interval if the data packet to be communicated has been presented to the first communication device (see Friedman col.5 lines 31-36; col.8 lines 1-14); and

means for translating the predetermined portions packet header information for the data packet according to a cipher algorithm seeded by the cipher key (see Friedman col.5 lines 22-30; col.7 lines 59-61; col.11 lines 14-16).

As per claim 51, Friedman discloses a device for securing packet header information as set forth in Claim 50, further comprising:

means for queuing the data packet until the cipher key has been derived (see Friedman col.5 lines 46-51).

As per claim 52, Friedman discloses a device for securing packet header information as forth in Claim 48, wherein the wide area network is the Internet (see Friedman col.2 lines 31-33). (Examiner takes specific note of paragraphs 3 and 4 of Applicant's *Specifications* wherein Applicant provides sufficient evidence that it is well known in the art that the Internet is the largest WAN in existence and has become an integral part of the missions of a wide variety of organizations who connect their networks to the Internet in order to share information with the cyber world in general as well as remote organizations with which they interact).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

April 8, 2005
TT

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER